UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/758,818	01/16/2004	Raynold M. Kahn	PD-200292	6585

20591 7590 08/21/2008

THE DIRECTV GROUP, INC.
PATENT DOCKET ADMINISTRATION
CA / LA1 / A109
2230 E. IMPERIAL HIGHWAY
EL SEGUNDO, CA 90245

EXAMINER	
SCHMIDT, KARL	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
08/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/758,818	KAHN ET AL.	
	Examiner	Art Unit	
	KARI L. SCHMIDT	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 June 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/25/2008, 7/15/2008, 7/18/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/12/2008 has been entered.

Notice to Applicant

The examiner notes that claims 1-48 are pending for examination. Claims 47-48 have been amended, to correct dependency.

Response to Arguments

Applicant's arguments filed in request for continued examination 6/12/2008 are based on the arguments presented on 5/2/2008, which have been fully considered but the examiner notes they are not persuasive for the following reasons:

The applicant argues that neither Raike, Son, Akiyama, nor Loisel disclose a single host receiver that is configured to perform multiple specifically claimed activities including decrypting and re-encrypting a media encryption key, transferring a re-encrypted media key to a client, receiving encrypted program materials that have been broadcast, and transferring received broadcast materials to the client. The examiner

disagrees. The examiner notes the combination of Raike in view of Son and Akiyama disclose the claimed invention. As the rejection shows, the examiner notes Raike discloses a method of distributing program materials received from a broadcast system between a host receiver and a client receiver for remote decryption (see at least, [0038]: the examiner notes consumers or end-users who wish to have access to encrypted media through the use of client devices (e.g. set-top boxes) is the client receiver and the retail server is the host receiver), comprising: encrypting a media key at the host receiver using a client key (see at least, [0038]); (d) transferring the encrypted media key form the host receiver to the client receiver, wherein the client receiver does not utilize a conditional access module (see at least, [0017]); (e) decrypting the encrypted media encryption key at the client receiver using the client key (see at least, [0018]); (f) receiving encrypted program materials from the broadcast system at the host receiver (see at least, [0007], [0009] and [0015]); (g) transferring the encrypted program materials from the host receiver to the client receiver (see a least, [0020]); (h) decrypting the encrypted program materials at the client receiver using the decrypted media encryption key (see at least, [0021]). Further Son was combined to disclose (a) receiving a encrypted data at the host receiver (see at least, [0027]-[0029]: the examiner notes that a store, decrypt and re-encrypt process may be performed on any data (e.g. media key)); and (b) decrypting the encrypted data at the host receiver (see at least, [0027]-[0029]: the examiner notes that a store, decrypt and re-encrypt process may be performed on any data); (c) re- encrypting data at the host receiver using a key (see at least, [0027]-[0030]: the examiner notes a public key encryption) and Akiyama

was combined to discloses conditional access system when each receiver apparatus has an individual master key (see at least, [0099]). Akiyama teaches that the conditional access system adopts a key configuration, as shown in, e.g., FIG. 3 (see at least, [0100]). More specifically the examiner notes a work key Kw (i.e. a pairing key) which is specified for each channel and is common to all receiver apparatuses is encrypted using an individual master key KM, and the encrypted key is sent. Furthermore, a channel key Kch is encrypted using that work key Kw, and the encrypted key is sent (e.g. from the Host) (see at least, [0101]). The examiner notes under the broadest reasonable interpretation the references in combination teach the claimed limitation. Further the examiner notes the references where combined and motivation was provided, and that one of ordinary skill in the at would have been able to combine the elements to yield predictable results. This argument is not persuasive.

With the argument to the argument of a "Single Host" the examiner notes the sections of Raike rely only on the use of client devices (e.g. set-top boxes) which is the client receiver and the retail server is the host receive (see at least, [0038]) r. Further the examiner notes Raike shows the "Single Host" performing the downloading of the media key to the client (see at least, [0051]: the examiner notes steering the information to the retail store for downloading to the user. The examiner notes this is not teaching away, due to the fact that the Host downloads the key to the client. Therefore the Raike reference discloses the use of a "Single Host." This argument is not persuasive.

With respect to the argument that Raike, Son, Akiyama, nor Loisel teach a host-receiver that can utilize a CAM module. The examiner disagrees. The examiner notes

Loisel discloses a host receiver that can utilize a CAM module (see at least, [0023]: the examiner notes the first device uses a CAM and the second device contains a decoder). This argument is not persuasive.

Further the examiner would like to note the applicant is arguing that the "Single Host" performs synchronization using a CAM to a receiver notes using CAM (see applicants arguments, page 15, 2nd paragraph) which is not in the claimed limitations. This argument is not persuasive

The applicant further argues that neither Raike, Son, Akiyama, nor Loisel disclose a client receiver that does not have a CAM that is configured to perform multiple specifically claimed limitation including decrypting a re-encrypted media encryption key and decrypting received program materials using the decrypted media encrypt on key. The examiner disagrees. The examiner notes Raike teaches a receiver that does not use a CAM module (e.g. the examiner notes a smart card slot). The examiner notes Raike teaches that the Client receiver receives a "just-in-time" key (see at least, [0041]) which is downloaded to the client receiver (see at least, [0017]). Further the examiner notes the "Single Host" can deliver (e.g. download) the media key to the client (see at least, [0051]), which shows a "Single Host" transferring a media key to a client without the use of a CAM due to the key being downloaded in real time. This argument is not persuasive.

Further the examiner would like to note the applicant is also arguing a thin client box configuration which in not claimed in the limitations (see applicants arguments, page 17-18). This argument is not persuasive.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-12 and 45-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Raike et al. (US 2002/0162104 A1) in view of Son et al. (US 2001/0017920 A1) and in further view of Akiyama (US 2002/0001386 A1).

Claims 1 and 7

Raike discloses a method of distributing program materials received from a broadcast system between a host receiver and a client receiver for remote decryption (see at least, [0038]: the examiner notes consumers or end-users who wish to have access to encrypted media through the use of client devices (e.g. set-top boxes) is the client receiver and the retail server is the host receiver), comprising: encrypting a media key at the host receiver using a client key (see at least, [0038]); (d) transferring the encrypted media key form the host receiver to the client receiver, wherein the client receiver does not utilize a conditional access module (see at least, [0017]); (e) decrypting the encrypted media encryption key at the client receiver using the client key (see at least, [0018]); (f) receiving encrypted program materials from the broadcast system at the host receiver (see at least, [0007], [0009] and [0015]); (g) transferring the encrypted program materials from the host receiver to the client receiver (see a least,

[0020]); (h) decrypting the encrypted program materials at the client receiver using the decrypted media encryption key (see at least, [0021]).

Raike fails to disclose (a) receiving an encrypted media encryption key at the host receiver; (b) decrypting the encrypted media encryption key at the host receiver; and (c) re-encrypting the decrypted media encryption key at the host receiver using a pairing key.

However, in an analogous art Son discloses (a) receiving a encrypted data at the host receiver (see at least, [0027]-[0029]: the examiner notes that a store, decrypt and re-encrypt process may be performed on any data (e.g. media key)); and (b) decrypting the encrypted data at the host receiver (see at least, [0027]-[0029]: the examiner notes that a store, decrypt and re-encrypt process may be performed on any data); (c) re-encrypting data at the host receiver using a key (see at least, [0027]-[0030]: the examiner notes a public key encryption).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike's media key to include (a) receiving a encrypted data at the host receiver; and (b) decrypting the encrypted data at the host receiver (c) re-encrypting data at the host receiver using a key as taught by Son. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide a extra level of cryptography on the actual media key in order to make it more secure (see at least, Son, [0030]).

Raike in view of Son fails to disclose the use of a pairing key for content between the host receiver and the client receiver.

However, in an analogous art Akiyama discloses conditional access system when each receiver apparatus has an individual master key (see at least, [0099]). Akiyama teaches that the conditional access system adopts a key configuration, as shown in, e.g., FIG. 3 (see at least, [0100]). More specifically the examiner notes a work key Kw (i.e. a pairing key) which is specified for each channel and is common to all receiver apparatuses is encrypted using an individual master key KM, and the encrypted key is sent. Furthermore, a channel key Kch is encrypted using that work key Kw, and the encrypted key is sent (e.g. from the Host) (see at least, [0101]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike in view of Son's re-encrypted media key to include the use of a pairing key as the tool for encrypting content between a host receiver and a client receiver as taught by Akiyama. One of ordinary skill in the art would have been motivated to combine the teachings in order to minimize transmission volume by the use of a paring key (see at least, Akiyama, [0100]).

Claims 2 and 8

Raike fails to disclose further comprising decrypting the encrypted program materials at the host receiver using the decrypted media encryption key.

However, in an analogous art Son discloses further comprising decrypting the encrypted program materials at the host receiver using the decrypted media encryption key (see at least, [0031]-[0032]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike's media key to include further comprising decrypting the encrypted program materials at the host receiver using the decrypted media encryption key as taught by Son. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide a extra level of cryptography on the actual media key in order to make it more secure (see at least, Son, [0030]).

Claims 3 and 9

Raike in view of Son fails to disclose further comprising receiving the pairing key from the broadcast system at both the host receiver and client receiver.

However, in an analogous art Akiyama discloses conditional access system when each receiver apparatus has an individual master key (see at least, [0099]). Akiyama teaches that the conditional access system adopts a key configuration, as shown in, e.g., FIG. 3 (see at least, [0100]). More specifically the examiner notes a work key Kw (i.e. a pairing key) which is specified for each channel and is common to all receiver apparatuses is encrypted using an individual master key KM, and the encrypted key is sent. Furthermore, a channel key Kch is encrypted using that work key Kw, and the encrypted key is sent (see at least, [0101]). The examiner notes that the Kw is therefore both broadcasted and known at both the host receiver and client receiver in order for use with the Kch and KM.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike in view of Son's re-encrypted media key to include broadcasting the pairing key from the broadcast system at both the host receiver and the client receiver as taught by Akiyama. One of ordinary skill in the art would have been motivated to combine the teachings in order to minimize transmission volume by the use of a paring key (see at least, Akiyama, [0100]).

Claims 4-5 and 10-11

Raike fails to disclose the use of a pairing key and the host receiver and client receiver decrypting the pairing key using uniquely associated keys to both the host receiver and client receiver.

However, in an analogous art Son discloses decrypting the data using uniquely associated keys to both the host receiver and client receiver (see at least, [0030]: the examiner notes the use of a private key for server and subscriber station).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike's media key to include decrypting the key using uniquely associated keys to both the host receiver and client receiver as taught by Son. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide a extra level of cryptography on the actual media key in order to make it more secure (see at least, Son, [0030]).

Raike in view of Son fails to disclose the use of a pairing key for content between the host receiver and the client receiver.

However, in an analogous art Akiyama discloses conditional access system when each receiver apparatus has an individual master key (see at least, [0099]). Akiyama teaches that the conditional access system adopts a key configuration, as shown in, e.g., FIG. 3 (see at least, [0100]). More specifically the examiner notes a work key Kw (i.e. a pairing key) which is specified for each channel and is common to all receiver apparatuses is encrypted using an individual master key KM, and the encrypted key is sent. Furthermore, a channel key Kch is encrypted using that work key Kw, and the encrypted key is sent (see at least, [0101]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike in view of Son's re-encrypted media key to include the use of a pairing key as the tool for encrypting content between a host receiver and a client receiver as taught by Akiyama. One of ordinary skill in the art would have been motivated to combine the teachings in order to minimize transmission volume by the use of a paring key (see at least, Akiyama, [0100]).

Claims 6 and 12

Raike fails to disclose the use of a pairing key transferring the paring key from the host receiver to the client receiver.

However, in an analogous art Son discloses transporting a key from the source to the server via a communication channel (see at least, [0040]) and further from transferring the key from the server to the subscriber via a communication channel (see at least, [0030])

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike's media key to include transferring a key from the host receiver to the client receiver as taught by Son. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide a extra level of cryptography on the actual media key in order to make it more secure (see at least, Son, [0030]).

Raike in view of Son fails to disclose the use of a pairing key for content between the host receiver and the client receiver.

However, in an analogous art Akiyama discloses conditional access system when each receiver apparatus has an individual master key (see at least, [0099]). Akiyama teaches that the conditional access system adopts a key configuration, as shown in, e.g., FIG. 3 (see at least, [0100]). More specifically the examiner notes a work key Kw (i.e. a pairing key) which is specified for each channel and is common to all receiver apparatuses is encrypted using an individual master key KM, and the encrypted key is sent. Furthermore, a channel key Kch is encrypted using that work key Kw, and the encrypted key is sent (see at least, [0101]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike in view of Son's re-encrypted media key to include the use of a pairing key as the tool for encrypting content between a host receiver and a client receiver as taught by Akiyama. One of ordinary skill in the art would have been motivated to combine the teachings in order to minimize transmission volume by the use of a paring key (see at least, Akiyama, [0100]).

Claims 45 and 46

Raike discloses wherein the client receiver does not comprise a tuner (see at least, [0038]: the examiner notes set-top boxes are not turners).

Claims 47-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Raike et al. (US 2002/0162104 A1) in view of Son et al. (US 2001/0017920 A1) and Akiyama (US 2002/0001386 A1) in further view of Loisel (US 2003/0026428 A1).

Claims 47 and 48

Raike in view of Son and Akiyama disclose all elements of the claimed invention however fail to disclose wherein the host receiver utilizes a conditional access module (CAM).

However, in an analogous art Loisel discloses wherein the host receiver utilizes a conditional access module (CAM) (see at least, [0023]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike in view of Son and Akiyama to include wherein the host receiver utilizes a conditional access module (CAM) as taught by Loisel. One of ordinary skill in the art would have been motivated to combine the teachings in order to allow for secret encrypted communication between paired devices (see at least, Loisel, [0002]).

Claims 13-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Raike et al. (US 2002/0162104 A1) in view of Loisel (US 2003/0026428 A1) and Son et al. (US 2001/0017920 A1) and Akiyama (US 2002/0001386 A1).

Claims 13, 22, 31, 36-38, and 43-44

Raike discloses a method of distributing program materials received from a broadcast system between a host receiver and a client receiver for remote decryption (see at least, [0038]: the examiner notes consumers or end-users who wish to have access to encrypted media through the use of client devices (e.g. set-top boxes) is the client receiver and the retail server is the host receiver), comprising: encrypting a media key at the host receiver using a client key (see at least, [0038]); transferring the encrypted media key form the host receiver to the client receiver, wherein the client receiver does not utilize a conditional access module (see at least, [0017]); decrypting the encrypted media encryption key at the client receiver using the client key (see at least, [0018]); receiving encrypted program materials from the broadcast system at the host receiver (see at least, [0007], [0009] and [0015]); transferring the encrypted program materials from the host receiver to the client receiver (see a least, [0020]); decrypting the encrypted program materials at the client receiver using the decrypted media encryption key (see at least, [0021]).

Raike fails to disclose wherein the host receiver utilizes a conditional access module (CAM) and receiving an encrypted media encryption key at the cam/host receiver; decrypting the encrypted media encryption key at the cam/host receiver; and

re-encrypting the decrypted media encryption key at the cam/host receiver using a pairing key.

However, in an analogous art Loisel discloses wherein the host receiver utilizes a conditional access module (CAM) (see at least, [0023]) and further pairing of the host receiver and CAM for a secure communication session (see at least, [0002]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike to include wherein the host receiver utilizes a conditional access module CAM as taught by Loisel. One of ordinary skill in the art would have been motivated to combine the teachings in order to allow for secret encrypted communication between paired devices (see at least, Loisel, [0002])

Raike in view of Loisel fails to disclose receiving an encrypted media encryption key at the cam/host receiver; decrypting the encrypted media encryption key at the cam/host receiver; and re-encrypting the decrypted media encryption key at the cam/host receiver using a pairing key.

However, in an analogous art Son discloses receiving a encrypted data at the receiver (see at least, [0027]-[0029]: the examiner notes that a store, decrypt and re-encrypt process may be performed on any data (e.g. media key)); and decrypting the encrypted data at the receiver (see at least, [0027]-[0029]: the examiner notes that a store, decrypt and re-encrypt process may be performed on any data); re-encrypting data at the receiver using a key (see at least, [0027]-[0029]: the examiner notes a public key encryption) .

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike's in view of Loisel's media key and (CAM) to include receiving a encrypted data at the receiver; and decrypting the encrypted data at the receiver re-encrypting data at the receiver using a key as taught by Son. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide a extra level of cryptography on the actual media key in order to make it more secure (see at least, Son, [0030]).

Raike in view of Loisel and Son fails to disclose the use of a pairing key for content between the host receiver and the client receiver.

However, in an analogous art Akiyama discloses conditional access system when each receiver apparatus has an individual master key (see at least, [0099]). Akiyama teaches that the conditional access system adopts a key configuration, as shown in, e.g., FIG. 3 (see at least, [0100]). More specifically the examiner notes a work key Kw (i.e. a pairing key) which is specified for each channel and is common to all receiver apparatuses is encrypted using an individual master key KM, and the encrypted key is sent. Furthermore, a channel key Kch is encrypted using that work key Kw, and the encrypted key is sent (see at least, [0101]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike in view of and Loisel and Son's re-encrypted cam/host media key to include the use of a pairing key as the tool for encrypting content between a host receiver and a client receiver as taught by Akiyama. One of ordinary skill in the art would have been motivated to combine the teachings in

order to minimize transmission volume by the use of a paring key (see at least, Akiyama, [0100]).

Claims 14 and 23

Raike fails to disclose further comprising decrypting the encrypted program materials received from the broadcast system at the host receiver using the decrypted media encryption key.

However, in an analogous art Son discloses further comprising decrypting the encrypted program materials received from the broadcast system at the host receiver using the decrypted media encryption key (see at least, [0031]-[0032]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike's media key to include further comprising decrypting the encrypted program materials received from the broadcast system at the host receiver using the decrypted media encryption key as taught by Son. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide a extra level of cryptography on the actual media key in order to make it more secure (see at least, Son, [0030]).

Claims 15, 18, 24, 27, 32 and 39

Raike fails to disclose receiving the first pairing key from the broadcast system at both the host receiver and the conditional access module (CAM) and the client receiver.

However, in an analogous art Loisel discloses wherein the host receiver utilizes a conditional access module (CAM) (see at least, [0023]) and further pairing of the host receiver and CAM for a secure communication session (see at least, [0002]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike to include wherein the host receiver utilizes a conditional access module CAM as taught by Loisel. One of ordinary skill in the art would have been motivated to combine the teachings in order to allow for secret encrypted communication between paired devices (see at least, Loisel, [0002]).

Raike in view of Loisel and Son fails to disclose the use of a pairing key for content between the host receiver and the CAM and the client receiver.

However, in an analogous art Akiyama discloses conditional access system when each receiver apparatus has an individual master key (see at least, [0099]). Akiyama teaches that the conditional access system adopts a key configuration, as shown in, e.g., FIG. 3 (see at least, [0100]). More specifically the examiner notes a work key Kw (i.e. a pairing key) which is specified for each channel and is common to all receiver apparatuses is encrypted using an individual master key KM, and the encrypted key is sent. Furthermore, a channel key Kch is encrypted using that work key Kw, and the encrypted key is sent (see at least, [0101]). The examiner notes that the

Kw is therefore both broadcasted and known at both the host receiver and client receiver in order for use with the Kch and KM.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike in view of Son's re-encrypted media key to include broadcasting the pairing key from the broadcast system at both the host receiver, CAM, and the client receiver as taught by Akiyama. One of ordinary skill in the art would have been motivated to combine the teachings in order to minimize transmission volume by the use of a paring key (see at least, Akiyama, [0100]).

Claims 16-17, 19-20, 25-26, 28-29, 33-34 and 40-41

Raike fails to disclose the use of a pairing key and the host receiver, CAM, and client receiver decrypting the pairing key using uniquely associated keys to both the host receiver, CAM, and client receiver.

However, in an analogous art Loisel discloses wherein the host receiver utilizes a conditional access module (CAM) (see at least, [0023]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike to include wherein the host receiver utilizes a conditional access module (CAM) as taught by Loisel. One of ordinary skill in the art would have been motivated to combine the teachings in order to allow for secret encrypted communication between paired devices (see at least, Loisel, [0002]).

Raike in view of Loisel fails to disclose the use of a pairing key and the host receiver, CAM, and client receiver decrypting the pairing key using uniquely associated keys to both the host receiver, CAM, and client receiver.

However, in an analogous art Son discloses decrypting the data using uniquely associated keys to both the host receiver and client receiver (see at least, [0030]: the examiner notes the use of a private key for server and subscriber station). Further the examiner notes this could be performed at the CAM.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike in view or Loisel's media key to include decrypting the key using uniquely associated keys to both the host receiver, CAM, and client receiver as taught by Son. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide a extra level of cryptography on the actual media key in order to make it more secure (see at least, Son, [0030]).

Raike in view of Loisel and Son fails to disclose the use of a pairing key for content between the host receiver, CAM, and the client receiver.

However, in an analogous art Akiyama discloses conditional access system when each receiver apparatus has an individual master key (see at least, [0099]). Akiyama teaches that the conditional access system adopts a key configuration, as shown in, e.g., FIG. 3 (see at least, [0100]). More specifically the examiner notes a work key Kw (i.e. a pairing key) which is specified for each channel and is common to all receiver apparatuses is encrypted using an individual master key KM, and the

encrypted key is sent. Furthermore, a channel key Kch is encrypted using that work key Kw, and the encrypted key is sent (see at least, [0101]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike in view of Loisel and Son's media key to include the use of a pairing key as the tool for encrypting content between a host receiver and a client receiver as taught by Akiyama. One of ordinary skill in the art would have been motivated to combine the teachings in order to minimize transmission volume by the use of a paring key (see at least, Akiyama, [0100]).

Claims 21, 30, 35 and 42

Raike fails to disclose the use of a pairing key transferring the paring key from the host receiver to the client receiver.

However, in an analogous art Son discloses transporting a key from the source to the server via a communication channel (see at least, [0040]) and further from transferring the key from the server to the subscriber via a communication channel (see at least, [0030])

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike's media key to include transferring a key from the host receiver to the client receiver as taught by Son. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide a extra level of cryptography on the actual media key in order to make it more secure (see at least, Son, [0030]).

Raike in view of Son fails to disclose the use of a pairing key for content between the host receiver and the client receiver.

However, in an analogous art Akiyama discloses conditional access system when each receiver apparatus has an individual master key (see at least, [0099]). Akiyama teaches that the conditional access system adopts a key configuration, as shown in, e.g., FIG. 3 (see at least, [0100]). More specifically the examiner notes a work key Kw (i.e. a pairing key) which is specified for each channel and is common to all receiver apparatuses is encrypted using an individual master key KM, and the encrypted key is sent. Furthermore, a channel key Kch is encrypted using that work key Kw, and the encrypted key is sent (see at least, [0101]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Raike in view of Son's re-encrypted media key to include the use of a pairing key as the tool for encrypting content between a host receiver and a client receiver as taught by Akiyama. One of ordinary skill in the art would have been motivated to combine the teachings in order to minimize transmission volume by the use of a paring key (see at least, Akiyama, [0100]).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KARI L. SCHMIDT whose telephone number is (571)270-1385. The examiner can normally be reached on Monday - Friday: 7:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on 571-272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kari L Schmidt/
Examiner, Art Unit 2139

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139